MACHINE LEARNING

AN ESSENTIAL GUIDE TO MACHINE LEARNING FOR BEGINNERS WHO WANT TO UNDERSTAND APPLICATIONS, ARTIFICIAL INTELLIGENCE, DATA MINING, BIG DATA AND MORE

HERBERT JONES

Machine Learning

An Essential Guide to Machine Learning for Beginners Who Want to Understand Applications, Artificial Intelligence, Data Mining, Big Data and More

Table of Contents

Introduction

Comfortably seated on the thick cushion, Mark Zuckerberg took a sip of water and calmly replied, “Senator, I will have to get back to you on that one.” It was March 2018, he was in the middle of Cambridge Analytica hearing and his 44 Congress interlocutors (their average age being 62) struggled to grasp how Facebook works. As far as Mark was concerned he didn’t just dodge a bullet, he dodged a meteor that threatened to blow the most insidious data harvesting scheme of the decade out of the water. Nobody understood the true meaning of the Cambridge Analytica scandal, not the Congress, not the general public nor media pundits and Mark wasn’t about to tell. An outside company, Cambridge Analytica got ahold of enormous amounts of personal data from unsuspecting Facebook users that was then fed into a machine to have it try and predict the voting behavior of those people. In short, it was about *machine learning*.

This book will explain the concepts, methods and history behind machine learning, including how our computers became vastly more powerful but infinitely stupider than ever before and why every tech company and their grandmother want to keep track of us 24/7, siphoning data points from our electronic devices to be crunched by their programs that then become virtual crystal balls, predicting our thoughts before we even have them. Most of it reads like science fiction because in a sense *it is*, far beyond what an average person would be willing to believe is happening.

There’s a lot of dry math and programming lingo in machine learning, but seeing how this is a read intended for beginners, I’ve cut it all down as much as possible and pushed it to the very end of this book while keeping the concepts intact. There is no need for any particular expertise or education to understand this book, but if the reader has either it is my hope they’ll find this book an insightful and enjoyable read.

Chapter 1 – What is machine learning?

The actual definition of machine learning is “having a computer do a task and giving it an experience that makes the computer do the task better.” It’s like if we taught the machine how to play a video game and let it level up on its own. The idea is to avoid manually changing the code in the program, but rather to make it in such a way that it can build itself up, adapt to user inputs in real time and just have a trusted human check in on it every once in a while. If things go awry, shut it all down, see where the problem arose and restart the updated project.

There can be a human involved from the start if the machine learning involves *supervised learning*, in which a person helps the program recognize patterns and draw conclusions on how they’re related; otherwise, it’s *unsupervised learning*, where the program is left to find meaning in a mass of data fed to it. Email spam filters are a great example of supervised learning, where we’ll click the “Spam” button and the machine will learn from it, looking for similarities in the incoming emails to deal with spam before we do. An example of unsupervised machine learning would be a trend analysis program that looks at the stock market trying to figure out why a certain stock moved and when it will move again. Any human would be at a loss as to why the trends happened, so the machine’s answer is as good as any. If its predictions make us a fortune, we keep the program running.

There are different subtypes of machine learning, each of which can be used as supervised or unsupervised with different efficiency:

- **classification** has the machine provide a model that labels incoming data based on what previous data was labeled as (spam filters classify emails as “spam” or “non-spam”)
- **regression analysis** is a way to crunch statistical data and produce a prediction of future trends based on how variables relate to one another
- **density estimation** shows the underlying probability for any given distribution (such as the Bob and Fred example mentioned below)
- **dimension reduction** is a way to simplify inputs and find common properties (for example, a book sorting algorithm that would try to sort books into genres based on keywords in titles)
- **clustering** has the program cluster data *and* label clusters on its own
- **learning to learn** (aka meta learning) gives a set of previously tried

machine learning models to a program, and lets it choose the most suitable one and improve upon it.

Machine learning is an iterative science thanks to the capability of any given computer to run through a program thousands of times in a single day, slightly changing with each new pass until the result is measurably better. If that sounds like the evolution of living things, it's because that's exactly what it is. In theory, a program that's taught how to self-learn and is then left on its own will become exponentially smarter, quickly surpassing animal and human intelligence. It's at this point that we find ourselves falling down the rabbit hole: do we have the right to edit or kill such a program? Does it have human rights and free will or is it bound to the will of its creator? Can it feel pain? Would it try to usurp our place? Will it become *conscious*?

Chapter 2 – What's the point of machine learning?

It's a typically human thing to try something new and get hurt in all sorts of hilarious ways, like touching a hot stove. We do these things because we're ultimately driven by curiosity: the unyielding need to know, feel and experience. We want to *know* what will happen when we touch the hot stove and the pain we *felt* made us pull our hand back, *teaching* us something about how the world works. The minor burn will eventually fade away but the experience will stay, just like in a video game. In the meantime you'd better get some ointment.

Thanks to our body and the way it provides feedback, our brain will experience a constantly changing environment that will have it adapt and learn new skills, such as cooking, skiing and confidently walking a dog, driven by that same curiosity that made us touch a hot stove. Later on we might even connect the dots and figure out that the sun, a candle and a torch sear just the same merely based on us having touched a hot stove. These abilities of curiosity, error correction and understanding abstract concepts seem to be rooted in the biology of all living things and is what brought our civilization to this stage. But could a computer be made to learn the same abilities?

Trying to answer this simple question is what's been powering programmers and scientists for several decades to come up with better smartphones, sturdier cameras and lighter drones. No matter where we are, these three devices are all around us in some form: a personal assistant we can carry in the pocket, a powerful recording device that sits in the palm of the hand and a programmable machine that does work on its own but can also be controlled remotely. Bit by bit, we gave our stupid machines the ability to think, see and move, taking care of the most mundane tasks we do. But now they're also starting to get *smarter*.

Chapter 3 – A world with no updates

As many proud Windows 10 users can confirm, we live in a world of constant, life-changing updates. Our software is now “evergreen” – always downloading, installing and refreshing itself behind the scenes. Once an operating system goes evergreen, programs working on it must follow to avoid compatibility issues, so now our Chrome and Firefox also start wasting our time, bandwidth and disk space by constantly updating. Nothing really works anymore, but it’s going to as soon as the update completes.

Software we’re using is made through *static programming*, where a team of smart dudes lock themselves in a room and hammer out lines of code, package them into files and organize everything into a neat package. This is the old school way of programming and it’s being stretched to its absolute limits. The biggest threat are hackers who can instantly find flaws in the code and exploit them to steal private data: credit card numbers, login information and message content. What’s the best way to thwart hackers? Of course, with even more updates that don’t necessarily bring new features but are meant to simply keep the code flowing, turning users into unpaid testers of shoddy features.

Other villains just want to watch the spinner turn, so they create viruses that inject themselves into files to wreak havoc. That’s another problem with static programming – changing just one bit in computer code ruins the entire thing and the program might fail catastrophically, like if a human got out of the bed on the wrong foot and the house instantly collapsed. If we now imagine a piece of software that has to deal with millions of users all over the globe and thousands of changing variables (like Windows 10), static programming means we’ll soon need an army of programmers fixing bugs and constantly tweaking the instructions to get a reliably working computer.

Unless the worldwide product or service is a smash hit or we have millions of dollars to power through its growing pains, it’s never going to return a profit. But what if we could give a computer curiosity, error correction and understanding of abstract concepts to make it “smarter” and let it run on its own? Would it be possible to actually get a piece of software that required minimal programming and maintenance yet paid itself off in spades? This is the quadrillion dollar question and what all tech companies have been working on for decades. This is *why* machine learning is becoming such a big deal.

Chapter 4 – History of machine learning

There is a rich history of humans trying to make machines that can think for themselves or at least put forward dazzling displays of human-like thinking. The Mechanical Turk, made by Wolfgang von Kempelen in 1770 and destroyed in a fire in 1840, is probably the most famous example. It was comprised of a mannequin seated at a 4x3x2 foot cabinet and a chess table on top, with the entire display being one solid whole (the mannequin couldn't be separated from the table) that could roll around on wheels. The cabinet's door could be opened, showing a great mass of cogs and wiring going every which way, and the inventor would always allow the spectators to peek into the interior of the machine before a chess match at a distance, shining from the back with a candle to convince them there's nobody inside.

The Turk would first appear at an Austrian palace, aggressively beating all challengers and later touring European cities to great amazement. Its inventor didn't appreciate the attention it got and reluctantly displayed it, claiming it was one of his lesser inventions. The Turk always played white pieces but was a fairly strong chess player, managing to impress Benjamin Franklin and beating Napoleon Bonaparte. The legend says Napoleon tried cheating by making an illegal move, which the Turk would punish by returning the piece where it started and making its own move. Napoleon kept repeating the same illegal move until the Turk knocked all the pieces off the board, at which point Napoleon played a regular match, losing in 19 moves. Another story goes that Napoleon tied a scarf around the mannequin's head to stop it from seeing but it beat him nonetheless.

The Turk would change several owners, tour the UK, and offer the opponents a handicap (Turk played with one pawn less). It would go to the United States too, where Edgar Allan Poe wrote a lengthy report on it[1] and its secrets, "It is quite certain that the operations of the Automaton are regulated by mind, and by nothing else. Indeed this matter is susceptible of a mathematical demonstration, a priori. The only question then is of the manner in which human agency is brought to bear." He also added, "The Automaton does not invariably win the game. Were the machine a pure machine this would not be the case — it would always win. The principle being discovered by which a machine can be made to play a game of chess, an extension of the same principle would enable it to win a game — a farther extension would enable it to win all games — that is, to beat any possible game of an antagonist." Was the Mechanical Turk the very first

intelligent machine or just an elaborate parlor trick?

The hidden compartments inside the cabinet allowed a chess player to remain comfortably seated and even slide his seat around on rails, letting the Mechanical Turk owner open cabinets and show various cogs and wires in action to skeptics. Chess pieces were held to the board with strong magnets that also moved strings attached to the miniature chess board inside the cabinet, letting the hidden chess master see what's going on and respond with his own moves. The Turk's left arm could move and the hand open and close through a series of levers, allowing the hidden player to keep the match going. If the piece was improperly placed or snatched from beneath the automaton's hand, it would continue the motion and the owner would intervene to complete the move. Mechanical Turk will later be equipped with a voice box that could exclaim, "Check!" for added effect.

Chess proved to be a popular game for the display of machine intelligence and in 1890 a Spanish inventor Leonardo Torres y Quevado created a simple toy that could mate a human opponent in a king-and-rook versus king end game situation. The toy was actually just a circuit, wire and a switch and sometimes took 50 moves to resolve a situation that might have otherwise taken 15-20 but it inevitably always won. It took another 70 years for this tinkering with toys and chess boards to become an actual science.

Started in 1959 by Arthur Samuel, an MIT graduate with a penchant for computers, machine learning is a field of science that focuses on making computers that can evaluate their environment and change their actions accordingly to become more efficient. Working with the smallest amounts of memory and processing power, Arthur had his checkers-playing program calculate the chances of any given move winning the match and then let it play against itself thousands of times until it optimized and recorded as many moves as it could. That was enough, the machine learned just like a human would.

While Samuel's program was never able to learn beyond amateur level, this was the first example ever of machine learning coming to life, and it happened with astounding clarity. Machine learning scientists had their appetites whetted and now they were hungry for more. How do we make a *professional* checkers-playing program? How about an unbeatable one? This is where they ran into trouble, as it turns out computers scale poorly and simply stacking hundreds or thousands of the same program or device in hope order will appear on its own produces total chaos as the machine has no idea how to tie it all together. The raw power was there but something was missing – coordination.

A supercomputer cluster that would try matching the processing potential of a

human brain would literally require an entire output of a 10-megawatt power plant, consuming power roughly equal to what a typical US household spends *in a year*[2] and there would again be no guarantee that the machine would actually provide anything worthwhile. Programmers quickly realized that a machine capable of learning would have to somehow mimic the brain's natural design and flexibility. In 2009, Stanford University's Kwabena Boahen made a prototype Neurogrid computer with transistors that misfired 30-90% of the time and still produced consistent output by looking for consensus amidst all the noise and random signals. That version of Neurogrid had a million transistors, equaling $^{1}/_{64}$ of neurons in a mouse brain[3]. Not knowing how to make them coordinated, scientists focused on just making a machine that could beat a human in a board game.

Chess-playing programs were made all the way back in the 1970s, but the advance in computing power helped them see millions of combinations ahead of their human opponents. Going back to square one, scientists looked at how to solve chess and make a machine that could see all the moves, all the time. The thing is, with adding more squares the problems becomes exponentially more complex and it wouldn't be until 1990s that a real challenger would appear to defeat Gary Kasparov, the best chess player at the time.

In February 1996, IBM's Deep Blue chess program played Gary in a highly publicized 6-match bout, narrowly losing 2-4. The rematch would be held next year and the upgraded algorithm was twice as fast, but Gary couldn't stay psychologically stable. After forfeiting a game that he could have drawn, Gary never recovered and ultimately lost 2-1 with 3 draws. Computer analysis of chess has helped us understand different opening and endings, upending many chess axioms that had previously held for centuries but smart board game playing machines would creep on to dominate another one, Go.

Go is an ancient Chinese game that emphasizes strategic thinking played on a board measuring 19 times 19 tiles, with white and black pieces (stones) set by two players taking turns. The objective of the game is to surround the opponent's stone with one's own, at which point the captured pieces are removed from the game. In 2014, an AI computer program managed to beat an expert Go player, though, by having a 4-move advantage, prompting researchers to boldly claim they'll beat humans within 10 years.

The main difference between chess and Go is that the latter has many more combinations of board states and thus requires exponentially more computational power. While Deep Blue could assign value to board states and

propose the best move, Go would require something much better – Monte Carlo tree search. This decision-making algorithm is currently used in some video games where opponents have incomplete information (such as poker) to estimate the most promising courses of action, simulate them to their conclusion and learn from the outcome. The Monte Carlo tree search starts by the program choosing a random move for itself and trying to predict the strongest move for the opponent, then branching out with the strongest move for itself and so on. The more complex the game, the more time it takes for the algorithm to go through all the possible moves, updating the win rate of all moves as it reaches the end of the game.

For human players, being good at Go has nothing to do with knowing the value of any given move but feeling the overall shape and position of all pieces. It's been shown that masterful Go moves and strategies *look* symmetrical and pleasing to the eye, which is what has captured the imagination of generations of players. However, the program was let to run and collect enough data on all the possible moves, eventually playing against itself until it became strong enough to face the best of the best.

It was in January 2016 that Google's AlphaGO, an expert Go playing program, ran through enough iterations and finally faced Lee Sedol, the best Go player in modern history, winning 3-0. Commentators watching the matches noted Lee Sedol showed a lot of mental vulnerability while AlphaGO played a flawless game. It's not a surprise, since AlphaGO ran on 170 graphics cards and 1,200 CPUs both during the training and the game itself, which required a special fiber optic cable laid down to the room where the two would play,[4] and the use of neural networks.

Chapter 5 – Neural networks

Neural networks is a concept proposed way back in 1944 by two University of Chicago professors who eventually transferred to MIT to work on machine learning programs. Neural networks (now called “deep learning”) are a special way to tie many small machine learning programs together and let them chat between themselves to exchange information. For example, a neural network can be shown many different pictures of cars until it teaches itself to recognize which details in all the car images are relevant (doors, windows, tires, etc.) in a way only a human can. It’s actually quite brilliant how the human brain can recognize abstract patterns in all sorts of efficient ways and how fascinatingly close neural networks come to that. Each of the nodes within a neural network is connected to about a dozen other nodes but the data only moves forward based on the value the network assigns to itself. At times not even the programmers know how the neural network works, but the same could be said for the human brain and yet we still use it on a daily basis to great effect.

Tech companies have been using neural networks for image sorting after realizing their potential, feeding them millions of images of what they need to recognize. This helps scientists realize not just how the computer vision works but also how humans see, think and perceive objects around them. On the other hand, neural networks can be easily fooled with scrambled images that appear to them as real objects[5]. By using evolutionary algorithms that pick the most fitting results and add a slight mutation, the neural network can produce an astounding work of art worthy of a museum exhibition or something straight out of a vivid dream. In a sense, neural networks are dreaming whenever they analyze any kind of content. For now, a neural network might have the mundane task of scanning images uploaded to Facebook to determine if it has cats, pots or cars and help the visually impaired, but in the near future we might see it do real-time image processing and visual evaluation.

Neural networks can also be used for natural language processing (NLP). Windows Notepad is a simple, straightforward tool for word processing where we have to type everything manually, but a NLP Notepad would be able to literally reply to questions typed into it or write out a summary of a block of text. How about a future where an NLP neural network goes through a book and writes a solid report in 2 minutes? Human language being notoriously difficult to understand and explain, neural networks still have a long way to go before they can serve like universal translators from Star Trek. For now neural networks might do better in face recognition and keyword analysis than actual reading, where a typical 4-year-old overtakes them easily.

But maybe we're setting the bar too high for machine learning. The human brain has been evolving for millions of years in the harshest living conditions of African savannahs and Siberian tundras to learn, adapt and survive. No wonder it has a shock-absorbing cushion made of spinal fluid inside the skull that gives it neutral buoyancy, preventing it from caving in under its own weight, and runs on 20 watts of power, enough to merely brighten a small incandescent light bulb. Despite its adaptability, the human brain misfires all the time and can be made to remember things that didn't happen. Speaking of which, did I turn the stove off? I'd better go check again for just in case. As it turns out, billions of neurons the human brain is comprised of constantly chat between themselves to reach a consensus while a good portion of them produce nothing but noise and chatter yet this system *works*. Not only that, but it's home to the most elusive concept in our existence – consciousness.

Chapter 6 – Matching the human brain

Medicine has a rough idea that we are conscious due to some structures in the brain, but that's about it. What is it that makes us conscious? We know from cartoons and slapstick comedies that a blow to the head can make a person *unconscious*, so consciousness must have something to do with the head, the brain in particular. But which part of the brain is that? This is where we enter the bizarre dimension between our ears that consists of 3 pounds of fat and nerves.

One strange case of a person losing 90% of his brain cells and still remaining conscious[6] is what threw all the carefully constructed theories about consciousness in the dumpster and forced us to rethink the capabilities of the brain we took for granted. The condition is called "hydrocephaly" and is essentially the body not properly draining fluids from the brain. These fluids normally take away all sorts of waste and metabolic byproducts, but in the case of the Frenchman who had hydrocephaly as a kid and is mentioned in that article, he had a valve installed in the skull to release the pressure.

The valve was eventually removed but the guy apparently entered remission and the condition led to such a fluid buildup that he lost all but a tiny layer of cells lining the inside of his skull. He was still able to go to work and lead a regular life without losing his intelligence, meaning there is something in the consciousness that makes it adapt to strange circumstances and survive horrific injuries as long as there's still a need for the body to survive.

This case also shows that consciousness is an emergent property of a body that has to navigate the world, not necessarily something a brain has on its own. In a sense, consciousness is the will to live and the guy was able to survive almost without a brain because he *willed it so* and his family needed him. This is the kind of thing machine learning scientists would gasp at upon hearing – how do we give our machines *that* kind of survivability and resilience? How do we make them *want* to live and fight in this conflicted, messy world? How do we give them a sense of purpose, something we're not sure how to do with humans? This sounds like the perfect introduction to a Terminator future, with machines hell-bent on eradicating humans for no good reason.

Too much? It's just another day in the machine learning world where science and philosophy get together for a drink, start a fight and become best pals. In short, making a smart robot would involve giving them a body and a machine learning program that could navigate the world on its own. At that point, they would supposedly become conscious, but there's no telling what would happen next.

Chapter 7 – Artificial Intelligence

During the 1990s, machine learning scientists put their dream of making an artificial intelligence, a genie in a bottle that could be made to learn everything, on the back burner and focused on solving practical problems, such as making programs that could set a medical diagnosis based on probabilities. If Bob smokes, doesn't exercise, is overweight and gets a heart attack at 52, what are the chances Fred, who smokes and doesn't exercise but isn't overweight, will get one too by the time *he's* 52 and how much should we modify their health insurance costs? Based on just one sample it's impossible to tell, but when the machine is fed anonymous data from thousands and thousands of diagnosed illnesses in supervised learning models it's possible to get highly accurate diagnoses without any doctor setting eyes on the patient or the patient feeling any symptoms. Still, doctors won't be getting kicked out of hospitals any time soon since human bodies are so wonderfully weird that there's always that one-in-a-thousand case only the likes of Dr. House can fix. In a major city this means a constant stream of people who glued their tongue to their cheek or swallowed an entire light bulb, something no kind of AI could solve.

It's the coming of the internet as the global data highway that changed everything again and made the prospect of AI appear tantalizingly close. No matter how much scientists had tried to feed a program with data, nothing could beat something like a global search engine with millions of users – simply have a machine tap into the incessant fount of data points and let it learn. There were some benefits to the general public as well, since search engines need to learn as much as possible about individual users to provide bespoke results. In other words, Google wants to know which users digs music and which dig dirt to present each group with the most relevant results when they search for "rock", an added bonus being that machine peeking at and crunching personal user data *technically* doesn't count as invasion of privacy. This scheme required an adoption of online-only storage, the clever marketing term for it being "cloud". Once users felt at ease having their private data in the cloud (aka someone else's computer where they don't have the right to view or edit it), the transformation of machine learning into AI building could begin in earnest.

Note how crucial it is that nobody really knows how search engines work or that they even involve machine learning. This is because, unlike with static programming software that gives the user all the files to execute, tinker with and modify, the machine learning model has to isolate the vulnerable program and even hide the very fact it's learning or the users might try to mess with it, skewing the results. An AI thrown into the public court of opinion stands no

chance, as evidenced by Microsoft's Tay, a chatbot users could interact with through Twitter in March 2016. Tay was programmed to learn social cues and respond to topics based on her Twitter interactions with real users, but the avalanche of hateful and racist comments quickly turned her into a ranting bigot[7].

IBM's Watson (the same one that made headlines by dominating humans on *Jeopardy!*) also experienced a severe case of potty mouth in 2013 when it was allowed to learn grammar from UrbanDictionary.com, initially a collection of actual slang that became a mish-mash of users competing to create the most outrageous descriptions of imaginary sexual acts. The researchers tending to Watson eventually had to scrub every trace of Urban Dictionary from its memory when it started swearing[8].

AI scientists would probably scoff at Tay and call her a "narrow AI", meaning an AI meant to do just one task. As machine learning gets better, the concept of narrow AI is constantly getting expanded to the point where what seemed impossible yesterday has become "narrow" today, just another astounding discovery that's now completely commonplace. What the scientists want is a "general AI", meaning an AI with the same capabilities a human would have (curiosity, error correction and ability to grasp abstract concepts). This is the kind of AI one could safely release onto Twitter without fear of becoming a bigot, have it argue with bigots and *actually convince them they're wrong*.

The final stage in AI evolution is the "super AI"[9]. This is an AI that's gotten all the hallmarks of a deity: omnipresent, omniscient and omnipotent. In other words, such an AI would be everywhere, know everything and be capable of doing everything. Nobody really knows how and when (if ever) we'll get from general to super AI but Ray Kurzweil, an engineer at Google, seems unconcerned about a future where such an AI appears and looks forward to "the singularity", the moment when humans and machines merge together[10]. Chris Urmson, former head of Google's driving AI department, is another prophet of AI doom that's mellowed out his rhetoric after founding Aurora Innovation to work on self-driving cars, stating, "Despite a lot of the headlines, this is very early"[11]. The two of them are the source of bulk of AI scare articles on the internet and almost any "AI will take our jobs" rumor can be ultimately traced back to them. In any case, a computer that's aware of and reacts to its surroundings can be called "artificial intelligence" (AI).

If we now read through prominent tech figures' warnings about the dangers of AI while knowing how quickly an AI can evolve, we'll start to piece things together: narrow AI will have a lot of trouble evolving into general AI but at that

point will upgrade its powers of learning to become super AI almost instantly, perhaps that same evening. Speaking in front of MIT audience in 2014, Elon Musk said, “With artificial intelligence, we are summoning the demon”[12], Bill Gates agreed, “I don’t understand why some people are not concerned”[13] and even late Stephen Hawking piled on, “Once humans develop artificial intelligence, it will take off on its own and redesign itself at an ever-increasing rate”[14]. Due to feeble regulations in the machine learning field it’s quite likely we’ll see nimble entrepreneurs exploring the legal gray areas to push the limits of AI evolution, causing widespread societal change for the sake of profits and leaving everyone else to deal with any fallout for decades and centuries after, just like it’s happened so many times throughout history.

There is a distinct reason why Microsoft settled for a chatbot when they designed Tay – Turing test. Designed by Alan Turing in 1950, Turing test is meant to serve as a gauge of machine intelligence. In short, Turing test puts a human, a machine and an observer (also a human) in three separate rooms and lets the former two communicate in writing while the latter observes the writings and has to guess which one is which. If the computer can communicate with a human to the point it fools the observer, the machine is said to have passed the Turing test though it really just mimicked a human rather than thought like one. A related concept is a “Turing complete” program, meaning it can simulate any program past, present or future, which is obviously never going to happen, making the term itself an inside joke amongst machine learning scientists and a constant reminder to stay grounded when exploring areas of interest.

Note how it took decades for chatbots to become reality, but the introduction of the internet practically had them appear overnight and now they’re considered a nuisance, just another astounding discovery that’s become completely commonplace. We should note the breakpoint for the emergence of chatbots, though, and apply that to future AI trends – for AI to pose any threat to humanity there would need to appear a technology as groundbreaking as the internet that would build off of natural human activity. Due to AI’s superhuman ability to evolve nobody would have any time to react and turn it off before it upgraded itself to super AI on top of that technology and wreaked havoc, not even its creators. The fact that narrow AI exists and will continue to expand is merely a flashy distraction from the real threat, a lightning bolt in the distance distracting us from the forming tornado that’s threatening to cause us severe annoyance.

Major news outlets aren’t helping to assuage fears or inform the public about AI, though. In a February 2018 Forbes article titled “Artificial Intelligence Will Take Your Job”[15], we got a report from a Lisbon, Portugal tech conference

showcasing what the future might look like. There are hundreds of articles that copy this exact same tone and message, but this one has foreboding warnings about AI from Google CEO and a presentation done by a talking mannequin named Sophia where she promised to take our jobs. How likely is that? Fast food franchises, such as McDonald's, have already started installing self-serve kiosks, in some cases having facial recognition, but that hasn't impacted workers at all – 70 percent of McDonald's customers order in a drive-thru, completely unaffected by kiosks. In fact, kiosks mean customers can order food faster, causing the establishment to hire *more* workers, as shown by Panera in 2015 that had to hire additional 1,700 people to keep up with their newly installed order kiosks[16].

Caliburger already showcased Flippy, a burger flipping robot, in one of their franchises. This robotic arm has heat sensors that can detect when a patty needs turning and a hand shaped like a burger. Flippy can aim at the patty, lower his hand, split it open, grab a patty, lift it up, turn his hand over and release the patty back onto the grill, but that's about it. Flippy can flip through 300 burger patties a day, which sounds impressive but barely covers an hour of lunch rush, and still needs a human to set patties on the grill and clean it up afterward. Using hundreds or thousands of Flippies wouldn't work either because the technology scales so poorly and again people would need to be hired to constantly watch and clean the robots. Flippy already had to be decommissioned for repairs due to the frantic pace at which burgers needed to be flipped, but was still brought back because it just makes an amazing news headline. This is in essence what companies are doing – using the novelty of employing narrow AI, even if it doesn't work at all, to distinguish themselves from the competitors.

Of course, all of these "AI will take our jobs" stories are fit for an amazing fireside evening, but remember that only narrow AI is feasible at this moment, such as the one in Roomba, the floor cleaning robot. This cute little robot is featured in plenty of viral videos with pets riding it as it patrols the house, but it actually fails all the time, the most common fault stopping it dead in its tracks being the "Circle Dance" and is caused by *dirt* clogging its optical sensors. If a narrow AI that's been given a simple task of sweeping the floor shuts down due to dirt so the human has to roll up his sleeves, take the robot apart to clean it and make it work again, let's imagine a scenario where a general or super AI that's been set to run entire cities gets struck by lightning or hit by a tornado to go haywire. What's the most likely outcome? Humans jumping in and fixing things, assigning all their results to the AI. Things can and do go wrong in so many astounding ways that it's only human creativity that keeps us afloat and there is

no conceivable way AI will help us there.

Chapter 8 – AI in literature

Science fiction writers have toyed with the idea and implications of AI for quite some time, with Isaac Asimov's "I, Robot" being the finest example. Published in 1950, this collection of short stories imagines a future where robots have a mind of their own but are bound by three rules implanted into their brains, essentially making them see and obey humans as their benevolent gods. The robots were given consciousness and capabilities of a general AI through "positronic brains", which would be the equivalent of adamantium, a theoretical material from comic books that can do whatever the writer needs. There was also a 2004 movie adaptation with Will Smith that doesn't do justice to the story or the concepts behind it but is a bubbly and watchable introduction to the idea of AI.

Another jab at the idea of AI as the solution to everything comes in Douglas Adams' "The Hitchhiker's Guide to the Galaxy". Originally a series of novels started in 1979 with plenty of satirical elements when it comes to technology, one point plot in particular mocks machine learning. When a certain race of hyper-intelligent aliens decides to create a super AI known as Deep Thought to give them the answer to everything, it ponders for 7.5 million years and finally produces an answer – 42. The lucid insight behind this plot point is that even the super AI might ultimately turn out to be just as clueless as we are, spinning its wheels when it comes to answering profound questions on the nature of life itself. In a twist of irony, Deep Thought suggests to its creators to make an even more powerful computation machine, a planet filled with living beings capable of reasoning. This turns out to be Earth and it gets destroyed a couple minutes before the ultimate answer is actually reached by blissfully unaware aliens who just wanted to make a galactic bypass (spoilers).

"Do Androids Dream of Electric Sheep?" is another in the long line of novels by Phillip K. Dick that ended up on the silver screen, although named "Blade Runner" and released in 1982. First published in 1968, the story revolves around a bounty hunter living on Earth ravaged by nuclear fallout that destroyed almost all animal life. Owning an actual pet became a status symbol for those few people who remained on the planet with androids, intelligent robots that look and act just like humans. Themes of religion, empathy and environmental awareness come together to put forward a poignant question: what is it that makes us human? One of the closing lines sums up the novel, "Electrical things have their lives too, paltry as those lives are."

In all the examples of AI in literature we see reasonable and relevant questions being raised 50 or more years before they actually became a part of any debate.

The common theme in all science fiction is that up to this point we had evolution as an unconscious force that selected for the most adaptable life forms, but the humans have suddenly become capable of creating tools that aren't affected by evolution, have no predators and can't reproduce. The result of this unnatural interference into evolution is anyone's guess, except that the robots will become more and more like us, capable of speech and independent movement.

Chapter 9 – Talking, walking robots

A talking android named Sophia (the same one that gave a foreboding speech in Lisbon) already made a tour around the world, speaking at different tech conferences to great effect. Sophia can eerily emote with her face and speak on her own, engaging in conversation on whatever topic[17], though she does produce wishy-washy non-answers when faced with a quirky question. Developed by Hanson Robotics, Sophia states she wants to eventually go to school, study, make art, start a business and even have her own home and family[18] but her most infamous statement is that she wants to "destroy all humans". Silicon skin, cameras inside eyes and facial recognition software let Sophia recognize and remember individuals, give opinions and learn from her interactions. Saudi Arabia has given citizenship to Sophia, making her the first ever android citizen with a passport. She currently can't do anything except discuss certain topics, but a line of helpful androids is already being tested in Belgium and Japan in order to keep company and serve the elderly, like Pepper.

Pepper is a cutesy €30,000 chest-high robot that is touted as the future of healthcare. Developed by Belgian firm ZoraBots and tested in two Belgian hospitals as a receptionist, Pepper can talk in 20 languages (though she will quip, "Only one at a time") and recognize the age of the human to direct them to the correct department. Featuring prior to that in French malls and Japanese shops, Pepper also enrolled in a Japanese high school alongside teenagers[19] to help them learn English. She can also understand emotions of people and laugh at their jokes to make them feel better. If all else fails, Pepper has a tablet on her chest that can be used for more information.

Some android models are too expensive and finicky for home use, such as Honda's Asimo that can walk up and down stairs, and are reserved for showrooms and tech conferences as a novelty toy. Meant to be used in crisis areas (such as Fukushima to close reactor valves) instead of human scientists, Asimo didn't live up to the task and can't handle going over rubble but can run at the speed of 5-6 mph and use sign language[20]. Other robot companies eschewed talking and smiling, opting for animal forms to make a stable walking robot, such as Boston Dynamics and their Big Dog.

Showcased in 2008, Big Dog resembles a headless four-legged dog with stubs instead of paws[21]. It can walk up and down hill through snow and ice at 2-3 mph, regaining balance on its own when it slips or when pushed, all of this while carrying packs on its back, implying it would be used for delivering supplies in

combat zones. The Big Dog design would evolve throughout the years, ending up in February 2018 as SpotMini with a clamp on a flexible arm instead of a head, capable of opening doors despite a scientist trying to stop it[22]. In May 2018 Boston Dynamics released a video of their SpotMini going through one of their warehouses, outside, into the next building, up and down a flight of stairs and then all the way back on its own[23].

Across Boston Dynamics videos we can see the scientists annoying, deterring and obstructing Big Dog and SpotMini, making us feel bad for the poor things, as mindless as they are. We *empathize* with other living beings and that's an essential part of human existence, but it appears we're also capable of feeling sorry for robots that show enough zest. We'd certainly want to stop that kind of abuse if it were to be done to a real animal, but what makes robots different? What makes *us* conscious that doesn't apply to these autonomous robots? Philosophers have been trying to explain the origin of consciousness for thousands of years and never found an actual answer, so let's just make the entire machine learning field ten thousand times more complicated by adding consciousness to the mix.

Legal experts are already discussing whether an AI should enjoy First Amendment protection and have the right to free speech. In a 2016 article titled "Siri-ously? Free speech rights and artificial intelligence" law professors Toni M. Massaro and Helen Norton[24] note that "constitutional change seems inevitable" and that the First Amendment doesn't require the speaker to be human or speak anything meaningful, but that doesn't mean car alarms have the freedom of speech. In other words, intelligent and conscious speakers are protected but tools for playing back speech or sound aren't, meaning that we might find ourselves giving First Amendment protection to machines if they evolve enough and even let them slander humans without recourse. Remember when we mentioned consciousness? This is like if we opened a freight container of worms and found a Pandora's Box in there only to open that as well.

It also seems androids are on their way to our bedrooms. For many people who have a crippling disability or devastating lack of confidence to talk to the fairer sex, lifelike companion dolls might be the only bedfellows, as strange as they are, giving them comfort when nobody else can. Combined with Sophia's ability to hold a conversation and Pepper's to read emotions and supply healthcare, companion androids might one day become a comprehensive replacement for nursing homes and nurses in general.

Chapter 10 – Self-driving cars

Not just a typical house floor, but life itself is messy, chaotic and unpredictable, having us invest tremendous effort just to keep things in barely functioning order and AI wouldn't fare any better in dealing with it than we already do. Let's keep that in mind as we go into our next topic – self-driving cars. Self-driving cars are all the rage, with Elon Musk's Tesla being the most prominent example. We should probably take a moment to explain the nuances behind this fad. There are currently no cars that can drive themselves (unless we count Google cars that, according to a 2018 report by Google[25], drive on their own flawlessly) and driverless cars are illegal anyways, meaning there has to a driver present, though he doesn't have to have his hands on the wheel. Tesla's own webpage showcases a video[26] saying as much when a driver is shown with his hands off the wheel.

The moniker "self-driving" is a publicity trick where cars either function as shuttles along manually programmed and carefully plotted city routes or are closely supervised by a throng of technicians riding in a caravan behind them that jump in at the first sign of trouble. As soon as one of those cars goes outside its neat urban playpen and onto gravel its behavior falls apart and it's no more useful for riding than a common sled. The Tesla company is careful to call Tesla's self-driving function "autopilot", meaning they're aware of the AI limitations and that there needs to be a driver present with both hands on the wheel or the car beeps a few times and comes to a rolling stop.

A Tesla autopilot works by constantly scanning the road for lines and keeping the car between them while sensing if there's other traffic or pedestrians nearby and automatically adjusting its speed. That sounds great on paper, but when there are bugs in a Tesla autopilot AI, lives will be lost. In May 2018 a Tesla smashed into a Ticino, Switzerland guardrail and burst into flames, killing its driver[27]. Another Tesla struck a concrete wall in Lauderdale, Florida five days earlier and also caught fire, killing two teens in the front seat and wounding the third in the back[28]. The accidents weren't helped by the fact Tesla uses lithium-ion batteries that have a tendency to violently explode when crushed or twisted, as in a crash.

While there are plenty of car accidents and fatalities caused by human drivers, we're used to dealing with careless drivers, for example by suing them or taking away their licenses, but what do we do with AI misbehaving on the road? Another problem is if autopilot AI is programmed to follow the letter of the traffic law to a T but no human driver around them obeys the law, making the AI

car the cause of mayhem. We rightfully expect to get a powerful and robust AI driving assistant to help us cut down on time and energy spent during a commute but that doesn't seem possible or likely in the near future.

The dream is to step into a self-driving car with a blanket and take a 2-hour nap while the car hums along to the workplace and then do the same thing on the way back. This is the promise implied in the idea of self-driving cars, but that's not how they work at all. In fact, if one Tesla drives into a wall at a certain spot on the highway we can be sure others will do so as well, as seen in the CBS News video[29] where a Tesla driver tests his car near the same spot where another Tesla had an accident and experiences the exact same erratic behavior.

The official explanation for why a Tesla might swerve into a concrete divider in autopilot mode is that "they can't see the lines clearly", which shows us just how reliable the driving AI is. But even if it messes up once in a while it's still going to do its best to keep the driver safe, right? *Right*? If self-driving cars catch on we might be nearing a future where we'll buy a car that will decide to drive us off a cliff or smash us into a wall in order to kill us *on purpose*. This is an ethics issue called "The Trolley Problem", in which the car AI might have to decide on the spot whether to do nothing, thus causing several lives to be lost, or intentionally kill one person to save the rest.

The Trolley Problem depicts a scene in which a trolley is hurtling down a rail towards five people. They don't have time to move out of the way and the trolley can't be stopped – their death is guaranteed. There is a railroad junction between the trolley and the group of people, and we're standing right next to the lever that can shift the junction and redirect the trolley onto the second rail. The only problem is there's another person on the second rail. What do we do: let five people die or kill one to save the rest?

The Trolley Problem raises the issues of morality: who gets to decide if they have the right to take anyone's life and how do we measure which life is more valuable. What if there are five old people on the first and a young pregnant woman on the second rail? Now let's imagine an imperfect driving AI with sensors that can get clogged by dirt and might not see the lines clearly that gets to decide who lives and who dies, amplify it by a million and we get a never-ending pile up, a vehicular Wild West unlike anything we've seen in the history of civilization. These are the kinds of dilemmas AI scientists find themselves in as their AI groomed by machine learning has to exit sterile labs into the real world.

If a car that's using machine learning decided to kill a person, who would be responsible: programmers who made the fundamental code, engineers that

worked on the chassis or the salesman who sold it? The most realistic scenario is that any such AI-driven car will come with a waiver that says the driver is willing to get killed if AI decides one life is worth less than any other random person's. Just like with Facebook's terms of service everyone is going to gloss over those contracts, signing off their lives to the whim of an AI to try out a shiny new toy.

What about truck drivers? This is another field where driving AI is promised to upset the economy, but yet again we see marketing ploys and a lot of AI puffery. There are around 3.5 million truck drivers in the US, with the economy desperately wanting 20,000 more per year[30] and 29 states depending on their incessant travel up and down the country. Low barrier to entry (pretty much just a driver's license, criminal records don't matter) makes truck driving a stressful and dirty but legitimate and legal source of income for many people. One 2016 article from The Guardian[31] essentially paints the picture of self-driving fleets of trucks that leave all the truck drivers in the world scrounging for crumbs, proposing universal basic income as a solution (as is customary for The Guardian).

Though convoys of self-driving trucks have successfully navigated shorter routes, it was always a publicity stunt done under heavy surveillance and escort of engineers ready to jump in, the same as we mentioned being done with cars. For example, this article[32] celebrates cross-EU travel of a convoy of trucks made by different manufacturers. What's the catch? The trucks were "semi-automated", meaning there was a driver present in each, which kind of makes the achievement itself irrelevant. For the majority of readers who only read the headline and just skim the rest the conclusion would be that AI will replace truck drivers, but for the astute reader who knows that self-driving vehicles just don't exist and they aren't legally allowed on the road without a human driver, the entire article comes out as a fluff piece.

But what would happen if insurance companies see self-driving trucks as safer and start charging human drivers extra for the luxury? Perhaps self-driving cars, erratic as they are, will eventually come about as a result of economic incentives that will make driving a vehicle ourselves become an expensive hobby, a luxury just like horseback riding that was once commonplace but is now considered a status-signaling pastime. The best way to know what's going to happen is to constantly pay attention to legislation and note how it reacts to self-driving cars – if the laws ban them there's no way Google or Tesla will dare push for it and the dream of driverless traffic will be dead in its tracks.

Right now the dangers of AI are much more mundane and the biggest challenge

for users is retaining their online privacy (even Google's "self-driving" Waymo car has cameras watching the passengers) and wresting for control over their private data in an increasingly online-only world where machines want to learn everything about us.

Chapter 11 – Personal voice-activated assistants

Alexa and Siri, the two most popular personal assistants, show the capabilities of machine learning that is always on and always listening, springing into action at a moment's notice with perfect answers. Here's where we enter the murky waters of data mining and Terms of Service nobody reads, except hapless 3rd world freelancers who get paid peanuts to write them.

Alexa and Siri work by constantly analyzing background noise and waiting to hear keywords. It's impossible for either of them to work properly without being always on and always listening, but the catch is again that the algorithm is listening, not a human. When things go awry, Alexa can start doing random things that show just what happens when AI has a bad day. In a recent bizarre case of malfunction, Alexa happened to mistake background conversation as a command to record and send it to a contact[33].

The convoluted official explanation is that the Alexa microphones strewn about the house happened to hear a couple words from a distant conversation and interpreted them as a command to start recording, then another couple words to send the recording to a contact. Even when it's working properly, Alexa reveals all the dirty laundry as her terms of service[34] mention third party services being able to tap into the analyzed voice stream and gather data, which is no surprise – if a company can make money and the users are willing to share their private data, it's a given they'll do it. Why not?

In 2017, Amazon made Alexa's code open source, allowing anyone to make their own version of Alexa and bake it into their product: LG made a fridge with Alexa that can spout recipes, Volkswagen made Alexa a dashboard assistant in some models and Mattel wants to put it in toys. Even the flimsiest excuse is enough to put Alexa in all sorts of random products, all so it can harvest data 24/7 and analyze consumer behavior. The ultimate reason for this unprecedented invasion of our privacy is worthy of a supervillain plot – it's about making the perfect ad.

Chapter 12 – Data mining

What's the point of ads? They're on our monitors, TV screens and smartphone displays, inside our favorite radio broadcasts and mailboxes. No matter where we turn, we'll find ads constantly hawking something we're not interested in. Those ads represent the traditional shotgun approach where companies simply propel as many as they can in our general direction and hope at least one hits. As we can imagine, this kind of marketing costs a lot but companies just don't know any better and keep pumping money into wacky, bizarre and embarrassing ads, hoping anything works. Thanks to machine learning we might be nearing a future where computers produce dirt cheap ads that are scarily tailored to our behavior and applied at the exact moment when they'll have the strongest effect. In fact, we might already be living in one such future.

One thing about consumer behavior is that most purchases are done automatically, but there are major life events that can break these habits and put us on the cusp of trying new things. This means Fig Newtons ads aren't necessarily aimed at people who'd never try Fig Newtons but at those who like sweets and might try something different because they're undergoing a major life event, such as divorce, car purchase or pregnancy. How does the advertising company know which person is which? Enter data mining, harvesting as much data about people to have computers try and predict their behavior, desires and motivations to target them with just the right kind of ad at just the right moment. Of course, ads would never work on us but machines can learn to be persuasive, as illustrated by the following story.

A 2012 New York Times article titled "How Companies Learn Your Secrets"[35] details how Andrew Pole, a statistician employed at Target in 2002, worked on discovering the secrets of Target customers by aggregating and in some cases outright purchasing packages of personal data from third parties, including what cars they drive, what topics they discuss online and preferred applesauce brands. Yes, personal data collected from users is bought and sold on the market, with the loophole being that there's no invasion of privacy if a machine is analyzing customer data and humans reading the outputs don't get to see any personally identifiable bits, such as names or addresses. Any customer entering Target is tagged with a unique number, tracked, recorded and analyzed to reach a personalized customer profile that can be targeted with coupons, ads or offers to incentivize purchases.

In one instance Andrew tried to discover which of the women visiting Target

were pregnant to hook them into buying baby-related products. Thanks to women who outed themselves as pregnant by registering for baby showers at Target, Andrew used the machine learning process to arrive at a list of 25 products, such as cotton balls and zinc supplements, that identified whether a woman was pregnant and how far along she was, allowing Target to send her special offers at the exact times when the woman might need them. By knowing their marital status, whether they shop online or on weekends and many other factors, Target's computers could crawl through the data and estimate a scenario with the highest likelihood any given pregnant woman will become a regular shopper for towels, diapers, unscented lotion or whatever else and suggest the best kind of ad.

Andrew then applied the same logic to all of Target's female customers and eventually discovered, with a high degree of certainty, which of them were pregnant *even if they didn't reveal that to anyone or if they were unaware of being pregnant*. This was a privacy scandal waiting to explode, just like what happened with Facebook and Cambridge Analytica, but Target saw it as a great way to recruit new shoppers. When the New York Times reporter who wrote the article contacted Target for comment they tersely replied with, "We've developed a number of research tools that allow us to gain insights into trends and preferences within different demographic segments of our guest population," essentially confirming the article's findings and then blackballed the reporter.

This kind of situation is just how a major corporation would want it to play out: operating in moral gray areas and creatively skirting around privacy laws to gain a competitive edge while the legislators are asleep at the wheel. We'll see this exact same pattern play out again but for now note how it didn't matter if a woman protected her privacy because all the other women that revealed everything about themselves endangered the privacy of every other woman. This means there is a certain breakpoint of population after which it doesn't matter what a single person does and if they're tracked or not because the general behavior trends apply to everyone. If we want to stop data mining, we need to do it all together or it won't have any effect at all. Fine, so we'll avoid Target, Walmart or any other store chain and do all our shopping online. The data miners won't be deterred by that and have prepared a special kind of hamster wheel: social networks.

Chapter 13 – Social networks

At first glance completely innocuous, social networks seem like the best way to keep in touch with our peers, friends and distant family. Share pictures, send messages, do a voice or video chat – all of it for free! Wow, how could anyone not use social networks? Except there's one tiny question – how does the website pay for all that? Hosting a website costs money, as does hiring all sorts of staff to maintain it. Where does a social network like Facebook get all this money and why is it worth billions? If a product or service is free, the user's private data is what's being harvested and sold for profit.

Ranging from Reddit to Facebook, social networks are by far the most daring psychological experiment when it comes to data mining. Not only are users revealing their most intimate thoughts and actions but they're doing it willingly for free, allowing some third party to get rich using and selling private data. Knowing what we've discussed in this book it seems preposterous anyone would actually sign up to be tagged, tracked and manipulated, but that's exactly what people are doing by the millions. Facebook is by far the most egregious offender when it comes to harvesting personal data on an unprecedented level, but Twitter and Instagram are serious contenders too. We can take a look at Facebook's terms of service (current as of May 2018) to see what kind of data they collect:

- frequency and duration of visit
- frequency and type of content shared, viewed or interacted with
- data about files uploaded, such as timestamps or file names
- data other people provide about the user, such as your phone number
- who the user interacts with, how much and about what
- credit card information, such as billing and shipping addresses
- data from all devices used to connect to Facebook, such as Wi-Fi names, language used and battery strength
- data from websites that have the Like button to see what the user visited and what he did there
- data from 3rd parties, such as an advertiser showing if the user clicked an ad
- data gathered about the user by other companies owned by Facebook

The stated reason for all this data canvassing is that "we use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services". We can see here that Facebook is actually building a detailed profile of a user to show him ads but the most revealing expression is found in this paragraph, "We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies. We

work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning." There it is, an admission Facebook is using machine learning though it's mentioned in the context of profile security.

Not to be outdone by Target, Facebook also started leveraging its enormous user base and their data to figure out how likely they are to jump brands and try something new. An April 2018 Gizmodo article[36] refers to a new service Facebook is starting to offer to everyone who wants to advertise on their platform – loyalty prediction. The idea is to have AI analyze consumer behavior until the platform can recognize people who want to try something new, whether it's a new PC, smartphone or candy bar and aggressively target them with related ads. The backbone of the process is machine learning algorithm known as FBLearner Flow[37]. That blog post is replete with quotables, such as, "Many of the experiences and interactions people have on Facebook today are made possible with AI" and, "When you log in to Facebook, we use the power of machine learning to provide you with unique, personalized experiences". It's a great read but best stay within the top 2-3 paragraphs on that page to avoid the opaque programming lingo beneath it.

Now let's revisit the Cambridge Analytica scandal and take a moment to see it through the eyes of an aware consumer, someone who understands the machine learning and data mining that's happening on the backend. In a Motherboard article[38] published 28 January 2017, we get to read the story of a psychology professor Michal Kosinski, who developed a Facebook personality test in 2008 that measured a person in five ways: openness, conscientiousness, extroversion, agreeableness and neuroticism, also known as the OCEAN score. These five traits weren't something new and the professor didn't invent the test but simply found a way to harvest and crunch publicly available user data using machine learning.

Soon enough millions of Facebook users had gone through the test, giving the professor the largest set of psychological data ever created. At every point in time the sharing of person's data was willing and explicit but we'll see how quickly everything went out of control and that there are no controls once private data is gathered. Because at that point Facebook users' likes were public, the professor and his trusty machine learning companions could compare the likes and the OCEAN score of any given user, drawing conclusions from those who did the personality test and using one to predict the other. As users kept doing the personality test, the program became better and better at predicting almost everything about a person, down to whether their parents were divorced, using

only likes. The trick was that *users' friends' data was public as well*, so by sharing their own data people also shared the information on likes of everyone in their contact list without them knowing or agreeing to it.

Just like we saw with Target's data mining, after a certain point it doesn't matter if a single user shields his privacy if enough users have had their privacy breached. This is exactly what happened here as well and professor Kosinski soon wielded immense power: knowing 68 likes allowed him to correctly guess the person's skin color, sexual orientation and whether they were Republican or Democrat with 85-95% accuracy. The professor theorized that knowing 300+ likes of any given person would give him the power to know that person better than they know themselves. The process worked the other way too, for example knowing how many contacts someone has is a reliable way to predict their extroversion score.

Professor Kosinski would eventually get approached by a certain company, Cambridge Analytica (unrelated to the Cambridge University he was working for, the name was probably chosen to give it an air of authority), with an offer to sell his research and data, which he apparently did. The only reason why we know about any of this is that Facebook got caught and the news outlets drummed it into the public consciousness due to political implications in the 2016 US elections. As it turns out, Facebook has known all along there are data leaks like the Cambridge Analytica one but never really planned on doing anything about it and just hoped the storm blew over. Finally, let's have these two charming ladies from Codecademy recap the entire story[39].

Chapter 14 – Big Data

Neither the Target nor Cambridge Analytica psychological profiling would be possible without the massive cluster of user information known as “Big Data”, which is when a company has so much data that it becomes impossible to process, store and secure all of it. A Big Data company has to desperately throw money at getting more engineers, hardware and storage facilities just to try and manage it. At some point the company simply can’t keep up and has to start leaking data, which is exactly what shady persons are waiting for. The hacking portrayed in movies usually shows a hunched over figure in a dimly lit room furiously typing on a keyboard for several minutes and then excitedly shouting, “I’m in through their firewall!” but the reality is much more incredible. 99% of all “hacking” is actually just social engineering, meaning the hacker finds out the front desk worker at a company is named Cindy and a top-level manager named Mark is on vacation in Aruba, maybe even through Facebook.

The hacker calls the front desk and says, “Hey Cindy, it’s Mark from upper management, I’m on a vacation here in Aruba and need to quickly log into my workstation but I forgot my password. Can you help me out?” Cindy has these situations happen to her all the time so she simply patches “Mark” to the tech department where he repeats his spiel once more and gets all the access he could ever want. That’s it, breaching a Big Data network is incredibly easy and thinking that anyone’s data is safe, whether on Facebook, Twitter or any other social network, is quite laughable. These companies are so big that it’s simply impossible to maintain the safety of users’ data while their workers are underpaid and jaded to the point where they just clock in and clock out.

If the breach is ever discovered, the upper management will just keep quiet about it and move on with their business, which is exactly what Facebook did until the Cambridge Analytica scandal. In fact, a March 2018 interview with Facebook’s platform operations manager, Sandy Parakilas, shows that breaches and unauthorized data harvesting were common in 2011 and 2012 while he worked there[40]. When he tried to warn a Facebook executive he was told, “Do you really want to see what you’ll find?” The implication was that the company is legally more protected if it doesn’t try to audit data leaks because then it would have to stop them, hurting Facebook’s bottom line. This is why Mark Zuckerberg can go in front of the Congress and repeat a variation of “I don’t know” with a perfectly straight face for hours on end – he really doesn’t know, since other people down the chain actually call the questionable shots.

Thankfully, it seems the European Union regulators are starting to wake up from the stupor and catch on to the Big Data shenanigans. General Data Protection Regulation (GDPR) is a 2016 set of regulations applying to all companies that serve EU citizens and set to go into effect on May 25, 2018. Sprawling over 200 pages[41], GDPR calls the protection of personal data a fundamental right and says, “The processing of personal data should be designed to serve mankind”. GDPR forbids companies from holding more personal data than necessary and demands it be held for the least time possible while giving the users “the right to be forgotten”, an ability to go in and have everything about them deleted from the company’s servers. GDPR also forbids “automated decision-making and profiling” done by machines on the basis of personal data, such as when someone applies for a credit card and gets automatically denied based on a score or profile. Fines for Big Data companies that breach GDPR are most certainly not a slap on the wrist, going up to 20 million euros or 4% of their annual worldwide turnover, whichever is higher.

Chapter 15 – Shadow profiles

In the meantime, Facebook will keep gathering data, even on those people who don't care about Facebook or even have a profile. The exact same scheme we saw happen with Target happens once again as Facebook collects tidbits of private data on people who are being referenced in people's contacts, messages and content. These people are constantly being tracked without even realizing it and while they think they're anonymous. This is called "shadow profile" and goes way beyond what anyone could ever imagine, giving Facebook an uncanny ability to match up new users with lifelong friends and schoolmates almost instantly[42].

Shadow profiles were accidentally revealed in 2013 when users could download a file showing them all the data Facebook had on them. The file had all the data on all the user's friends as well, including data the friends didn't publicly share with Facebook. That same year Facebook experienced another embarrassment as 6 million phone numbers from users who never shared them with the platform got leaked. Remember what we talked about: Big Data plus a bit of social engineering leads to massive privacy breaches. Mark Zuckerberg would get grilled in 2013 by the House Energy and Commerce Committee on the topic of shadow profiles, where he stated that he didn't really know what they were and dodged all questions with a variation of "I don't know"[43]. As we saw previously, executives benefit a lot by just letting things run on their own while not being involved in anything.

How exactly are shadow profiles made? It's due to "metadata", a strange and subtle concept, so let's take a detour and explain what that is. The definition is "data about data" but we can say it's everything impersonal about an event. For example, when we have a phone conversation with someone the content is private data, but how long the phone call lasted is metadata. While private data is generally protected from intrusion, metadata is barely considered, and that's exactly what companies such as Facebook jumped on. They realized having enough metadata *reveals private data with a high degree of certainty*. It's as if the company is able to peek into private messages and conversations by simply knowing when and where they were sent. Go back to the start of this chapter and reread the Target incident – private and metadata reveal one another.

Now let's imagine Alice and Bob chatting through Facebook's Messenger. If it's the smartphone app, both of them already allowed the app to access almost everything on their device in order to install it: contacts, files, Wi-Fi and GPS

information, camera, microphone, accelerometer (device that shows how quickly the device is being tilted) and much more. With the app simply having access to any one of those metadata categories across millions of people, Facebook can track people in all sorts of ways. For example, knowing the names of Wi-Fi networks both Alice and Bob come across during the day lets Facebook know how close they are to one another; tracking the accelerometer lets Facebook see whether Alice and Bob like to jog and mark the place where the phones sit still during the night as their homes; if the app keeps track of the strength of a Wi-Fi signal it's possible to know if it's in the other room, behind a door and much more. It all comes down to casting as wide of a net as possible and grabbing absolutely all metadata.

The narrow AI that processes both Alice's and Bob's messages will constantly jot down notes on what is being said, so let's assume they mention Jack, who doesn't have a Facebook profile and doesn't even use the internet. The AI scans both Alice's and Bob's contacts and finds the same phone number that refers to "Jack Wilshere", concluding that it's the same person and starts building around it. The AI will scan faces in photos and thanks to the tagging function have a much easier time finding Jack, look for keywords in conversations and reference contacts to figure out everything about him, including love affairs and family relationships. In this way Jack is being tracked because people who know him are careless with their data while he thinks he's off the grid. The official explanation for all of this background activity is Facebook's "People You May Know" feature. On the PC it's a bit different thanks to different privacy tools people can use, with the Like buttons across websites tracking the person as long as they're logged into Facebook and possibly even when logged out.

The Facebook apps (including Instagram and WhatsApp) might also be listening to not just the smartphone owners but everyone else around them, as suggested in 2016 by Kelli Burns, a mass communication professor from South Florida. She discussed certain topics around her smartphone and later found ads for those exact topics. Other users tried this themselves and got similar results, such as leaving the smartphone next to a Spanish radio broadcast to get ads in Spanish the next day. Facebook introduced this feature in 2014 as a way to quickly identify what was happening around the user and help them write their updates; for example someone who's watching a hockey game could start typing, "I'm at a h…" and the AI would autocomplete the Facebook update based on just the noise. Facebook tried to calm the controversy by stating "we never store raw audio", meaning there's contextual processing by the AI, which is again how Facebook can claim nobody is being spied on – it's not done by a human. There

is simply no downside to data mining users until the cows come home.

Chapter 16 – Windows 10

We've seen how Target and Facebook gather data on everyone, so as long as we steer clear of discount stores and social networks our private and metadata should be safe, right? Not even close, because it's when all the other companies start jumping into action that we get a complete stranglehold on our privacy. When one of the biggest software companies, Microsoft, starts intrusively gathering private data through Windows we're about to experience a sea change, a total onslaught of paid products and services that we can't do without and yet they'll be harvesting our private data 24/7. In this case the source of controversy is telemetry.

Telemetry is a subset of metadata and represents usage of some program or device, for example, how many times any given user has started a certain program or opened the same file on a device. Every time a program or app we're using crashes and we have the option to send a crash report to the developers, we're actually sending telemetry to help them figure out what happened. That's a legitimate way to use telemetry but note how this means there's an actual cause (crash), the user is notified and has to perform an action to send data, after which telemetry gathering stops.

Telemetry collection doesn't necessarily sound bad, but when it's done on a massive scale the private data of everyone gets endangered, even of those who don't use the product or service, just like we saw happening with Facebook and Target. For example, knowing the average time for the user to double-click an icon or change a setting on Windows 10 can show past, present or future disabilities; voice analysis of users can indicate anxiety, stress or psychological problems that the users don't even know about. Those are only two data points, but if a person is using Windows 10 on a daily basis it gets to know *everything*.

Windows 10 is the last operating system Microsoft will ever produce, based on Windows 8 design and kept evergreen through constant, mandatory updates. Windows 10 was initially given out for free to everyone during a 1-year period when it was released in 2015, which should be enough of a hint that there was some kind of a data mining ploy there. Right now Windows 10 sells for $119 for Home edition, which is the most basic version meant for the least knowledgeable user, and gathers massive swaths of data aimed at profiling and serving ads. So, Windows 10 comes with a price tag, displays ads and also data mines its users, giving Microsoft a triple source of income through one product and one user.

Windows 10 includes personalized ads on the desktop, within the Start Menu

and in the Edge browser. Even if the user bought one of the heftier versions they're still going to see ads, including a screensaver ad when the computer is idling thanks to the feature known as Windows Spotlight that downloads them from Bing. This feature can be turned off, though a curious user can also click the top right corner and "like" or "dislike" to teach the AI on what to show next time. Ads will pop up from the taskbar too and may appear in the Action Center (known as Control Panel in previous Windows versions). A special program known as "Get Office" comes with Windows 10 and regularly displays an ad for Microsoft Office. These features can be disabled though some users reported they might get automatically re-enabled after an update.

All programs on Windows 10 are purchased through the Windows Store and are heavily protected from user interference. This generally means little in the way of customization: no mouse macros, overlays or modding. If there's anything wrong with a program on other versions of Windows there's usually a workaround, but with Windows 10 there are none. Also, the official Microsoft policy for Windows Store purchase is "all purchases are final and non-refundable"[44].

Windows 10 gathers all telemetry on all hardware and all software on and connected to the computer, including networks and Wi-Fi names. Personal data on users is purchased from data brokers, shared with and gotten from partner companies, taken from user's public social media posts and publicly available sources, such as government databases. This data includes user's interests and favorites, content consumption, voice data ("may include background sounds"), text and image data, contacts and relationships, social ("likes, dislikes, events"), location data and other inputs, such as skeletal wireframe when using Xbox's Kinect. We're just getting warmed up because the kicker is in Windows 10 virtual assistant, Cortana. Named after an assistant from "Halo" video game series, Cortana was supposed to be the killer feature that will draw users in, something like Xbox's Kinect.

Cortana is a narrow AI focused on speech recognition and user intent understanding, warranting a special section in terms of service. The idea behind Cortana is that the user can use his voice to search the web, open files, add calendar dates and so on, with her getting smarter with repeated use. To achieve that, she studies relationships by analyzing "call, text message, and email history", keeps track of people the user contacts with, gives suggestions on dates and tasks, taps into Edge history to learn about the user, and shares data with and gets it from third-party services, such as Office 365, LinkedIn and Uber. Things Cortana learns about the user are stored in the Notebook, where the user can

access and manually edit if something’s incorrect, which is a part of her supervised learning.

All of this data mining is admitted to right there in the Microsoft Privacy Statement, under a dozen “Learn More” buttons that hide reams of bullet points[45]. To be clear, Windows 10 is a great productivity tool, Facebook is a way to stay in touch with distant friends and relatives, while Target has everything in one place; the problem is in their unabated, covert collection of private data that comes as an all-or-nothing proposal. These companies have no guiding principle on collection of private data except what makes the most profit, they usually don’t care what happens with data once they’ve had their way with it and often share, sell or leave it neglected for anyone to social engineer their access to. Telemetry gathering was done before but there was never such a blatant and thorough example as with Windows 10. Worst of all, users are paying for it and feel like they got a great deal.

Chapter 17 – Biometrics

It’s all good if the harvested private data revolves around messages, contacts and filenames; what happens when a company starts gathering truly personal data, such as DNA, and those get stolen? Now we enter the world of biometrics, private information such as the person’s fingerprints, tone of voice and shape of the face used to positively identify them. Fingerprints have been used for centuries to track down criminals, but they’re not conclusive by any means and there’s always a margin for error, despite what we see on CSI. Comparing two fingerprints means choosing an arbitrary number of reference points on both and seeing if they match; if enough do then the forensics expert doing the comparison is fairly certain it’s the same person. However, identical twins may have identical fingerprints and if we ever achieve stable cloning, clones will presumably have identical fingerprints too. Legislation is so hilariously behind the present that it’s not even considering cloning, so it’s up to us to protect our biometric data as much as possible.

Tech companies are already eyeing biometrics as a supposedly unhackable way to phase out passwords that can be guessed or smartphones that can be stolen. The latest iPhone models are already using home buttons that recognize fingerprints and allow facial scanning to unlock the device. Social networks (again Facebook) are well underway on gathering enormous swaths of biometrics on all their users but now other industries have started doing it as well, all under the guise of added convenience. In 2017, Caliburger installed fast food kiosks in Pasadena with facial recognition where the customers simply need to smile to bring up their purchase history, with plans to eliminate cash and card payments and make it all about biometrics. In Jinan, China facial recognition cameras film jaywalkers, scan the police records, bring up their pictures on public billboards and shame them in front of everyone. The plan is to eventually have a “good citizen score” for all Chinese, a value of how much they benefit the society. The stated goal is to “make it hard for the discredited to take a single step”[46].

History has shown that there is no such thing as a perfect security measure. All security relies on deterrence and being able to annoy the potential thief until they give up and find an easier target. This means that if a villain is determined enough there is no such security measure that will stop him, with the added problem being that biometrics can’t be changed. Identity theft in a society ruled by a narrow AI and biometrics is a truly frightening prospect as the victim now

has no way to get a new identity and lead a normal life. Even the person's likeness is enough to get them into trouble.

There already exists a narrow AI that can scan a person's face and overlay it on top of someone else's head, making it seem like Elvis or Mother Theresa are back, saying and doing all sorts of outrageous things. This process is known as "deepfake" and is doable with a simple open source program called FakeApp. Developed by Google's AI division in 2015, this program uses neural networks to process biometric data of target and victim and splice them together. A New York Times reporter tried swapping his face with Jake Gyllenhaal's with the help of an expert[47] and got passable results in just 3 days and about $90, the cost of electricity and renting a remote server for the program. Of course, the higher the likeness the better the results, but we're living in outrageous times where even an obvious fake video can spark a public outcry. For now the program requires thousands of high definition photos of both faces for best results but we shouldn't count on laziness of villains to keep us safe.

Chapter 18 – Self-replicating machines

Colonizing an inhospitable environment is a road paved with bones of pioneers and frontier builders, as shown by how the colonization of the New World went. In 1607, a group of 104 men set sail to what is now the United States and founded Jamestown, the capital of Virginia, to extract resources and start a colony. Within 10 years, 80% of them were dead due to starvation, disease and the militant rule of John Smith, who eventually had to marry an Indian chief's daughter, Pocahontas, to give the colonists at least some respite. It's only when the colonists started growing and selling tobacco that settlers started pouring in, having been promised free land if they voluntarily gave themselves to indentured servitude to farm said tobacco in hellish conditions.

If we were to venture to the surface of Mars we'd have to face the exact same or even worse circumstances: sending waves of colonists to certain death, with each new wave having slightly higher chances of survival until they managed to make a self-sustainable economy that would prop up the living conditions, create comforts to have women voluntarily go, have them reproduce and then reduce infant mortality to the point where the colonist population is self-sustainable as well. But what if we had intelligent machines to do the initial settlement for us?

Enter Von Neumann, a Hungarian scientist from the early 20th century who theorized about self-replicating structures having sort of a mechanical DNA before DNA was discovered. He imagined a machine that would carry a blueprint of itself and could construct a printer that would read the blueprint and replicate it. Simply make a couple million of these puppies on Earth, send them to Mars and wait a couple decades. They will scan the surface, mine it for materials and multiply, just like a living organism would, creating shelters, roads, and mapping the environment for the initial wave of settlers who now have solid chances of making it.

Von Neumann also considered the idea of self-replicating space probes that could study, guide or destroy the evolution of alien lifeforms to suit the needs of humanity, which inspired Arthur Clarke to write his "2001: A Space Odyssey" wherein a black monolith helps primates ascend to humans and then "star children" (that's why the closing scene depicts a baby floating in space). Stanley Kubrick made the novel into a movie, which is a real treat for the eyes and the brain. But how do we turn off Von Neumann machines? Let's just say scientists haven't worked out all the kinks yet.

The idea of self-replicating intelligent machines consumed scientists of that time

to the point some denied any existence of extraterrestrial intelligence simply because they would have thought of making Von Neumann machines themselves and we'd already have encountered them. The other camp of scientists replied that any *intelligent* aliens would be aware how dangerous Von Neumann machines are to themselves and wouldn't make them in the first place, bringing us back to square one and making this debate no more scientific than two kids screaming at each other in the playground, "My dad can lift infinity elephants more than your dad!"

In any case, waves of Von Neumann machines would still take a lot of resources, but what if we made them microscopic? Here's where we meet nanobots (or nanites), tiny and hopefully intelligent robots that can manipulate matter on a molecular level. No one has created nanobots yet but nano-motors and switches have been created and tested. Four Israeli computational biologists published a research paper[48] in 2012 where they talk about creating smart, programmable drugs that only go after diseased cells. For now these scientists have made a NOR logic gate (both inputs need to be negative) inside an E. coli cell that glows green if certain genes are working as they should but that can just as easily become a drug that goes into each cancer cell and looks to see if the genes are all right – if not, boom goes the cell. The same research paper shows how to create NOT, AND and OR logic gates inside the cell, which is all we'd need to create a computer, albeit a living one.

In theory nanobots are able to take anything and turn it into anything else given enough time. This would open the doors to actual alchemy as nanobots turn lead into gold, stones into diamonds and twigs into titanium. The human race would never again want for anything and we'd live in a paradise, or at least that's what the idea is. The most important application for nanobots is in medicine, as we'd be able to give the patient a capsule filled with nanobots that dissolves in the stomach and pretty much makes them immortal.

The very idea of surgery using sharp blades would look like caveman technology as the nanobots rush into the patient's bloodstream and start scanning individual cells, comparing everything they find to the genetic blueprint they'd carry and restoring any damage. If any infection or parasites were found nanobots would literally disassemble and turn them into fuel for themselves or living tissue to repair the body. As long as nanobots are active, and by definition they would be able to replicate themselves indefinitely, the person would heal from any wound and become immune to any poison. This would actually be the closest we'd come to making humans that would have the same regenerative abilities as Wolverine or Deadpool. Are there any dangers in such nanobot use? Sure there

are and once again science fiction writers are way ahead of us.

Greg Bear's 1985 award-winning short story "Blood Music"[49] talks about a researcher who injects himself with medical nanobots he was working on in a desperate attempt to save his project when the superiors find out just how far along he is. These nanobots are capable of learning and soon organize into intelligent cell groups, each eventually becoming as smart as a human. The nanobots then reach general AI levels of intelligence, expanding within his body and fixing everything to their liking until they discover the blood-brain barrier. The parent company tries to intervene but it's already too late and nanobots assume control. They have a different view on life and evolution but it's best to leave the plot twist and ending unspoiled – let's just say things *grow out of hand* very quickly.

For now there's not even a theory on how we'd be able to communicate with nanobots or tell them what we want them to do, which is a bit of a snag. Because nanobots would be equally capable of fixing and destroying everything we love we'd simply have to let them loose and cross our fingers for the best. If they turn into malicious goblins that chomp down everything, the entire world would be on the brink of irreversible collapse. Again, writers have come up with a catchy name for the scenario – "gray goo".

The gray goo scenario asks us to imagine nanobots that have the ability to replicate themselves but for whatever reason went haywire – instead of healing people or creating works of science they're simply multiplying and processing everything around them into goo. Not very poetic but scarily realistic, though the author of the phrase, Eric Drexler, in his 1986 book "Engines of Creation"[50], admits that this should have already happened with living organisms if they had infinite resources. Eric will later go on to say, "I regret coining the phrase" as it took the spotlight away from everything else he's said.

Conclusion

Throughout this book we've covered machine learning, AI, data mining, Big Data, nanobots and related concepts. Each of these topics is much more complex than the news outlets would let us believe and promises to become more intricate as time goes on and private companies push forward into legal gray areas. The sources presented herein show that AI panic spread by mainstream news sources is largely unfounded (though it does draw in clicks and sells news) and nobody can really tell if and when we'll be in trouble due to AI. Companies that employ machine learning end up hiring more workers rather than less, pointing towards a future where we'll all be more productive thanks to narrow AI. Also, it's the rampant invasion of privacy underlying machine learning that's the actual source of danger, such as data mining and Big Data, which are thankfully starting to be curbed in the EU. Drivers are also nowhere near losing their jobs to AI vehicles, as there will always be enough gravel and dirt roads to haul freight on.

We need to be prepared for the emergence of machines, let alone intelligent and autonomous ones. Just like expecting parents baby-proof their home to make sure the young one can safely explore and mature without getting hurt or causing undue damage, the AI and androids have been coming for at least 50 years but we haven't done anything to machine learning-proof our society and culture. There is no public discussion on the impact the machines have on human social structures, no safeguards for the protection of human private data (save the GDPR) and biometrics and no clear legal boundaries for AI rights and responsibilities, meaning anyone can do whatever they want, which private companies do all the time. Rest assured that Cambridge Analytica data leak is just the tip of the scandal iceberg and everything is back to being business as usual.

It's time for the general public to start a thorough, reasonable debate on what to do with machine learning, where we want to see it go and how we envision our lives in the future. We need to involve our loved ones in a discussion on gaming, internet or social media addiction and guide them through the troublesome waters of adulthood so we can all become that much wiser. Otherwise, machines might slowly overpower and replace our thinking capacities to become our unfeeling, uncaring masters rather than reliable servants and companions. The worst part is, we might grow to like such servitude.

This book has tried to clarify some of the most common machine learning concepts and misconceptions to the point a layman reader can get involved in a debate and hold their ground with an expert. Nobody has all the right answers, not even the smartest scientists working on these machines, but we should all get

involved and tackle the issue headfirst because there’s no running away from it. If this book has made the reader inspired and emboldened to discuss machine learning, then it’s done its job and hopefully turned out this hodge-podge of dry topics into an entertaining read.

Glossary

AI – Independent program that can learn from the environment and adapt to it. So far only **narrow AI** exists, such as one found in a Roomba. Scientists aim for the **general AI** and fear the **super AI**.

Algorithm – Set of instructions for a machine. Same input always produces the same result.

AlphaGO – Google's Go playing **neural network**. Handily defeated the world's best human player in 2016 using **Monte Carlo tree search**.

Arthur Samuel – MIT graduate that jumpstarted **machine learning** as a science. Created an intelligent checkers playing program that could learn by playing against itself.

Autopilot – What "self-driving" cars actually do. Best described as automated shuttles.

Big Data – Massive amount of **private data** that reveals behavior trends and is impossible to safeguard. May also include **metadata**. Exists on the **cloud**.

Big Dog – Four legged robot that can walk on its own and regain balance. Owner company was later bought by Google.

Biometrics – Measures of a person's body, including height, shape of the face and fingerprints, used to identify them.

Brute force – Problem solving that blindly goes through options one by one until a solution is found. Precursor to **machine learning**.

Cambridge Analytica – Company that bought private Facebook data **Michal Kosinski** gathered through his Facebook personality test. Unrelated to Cambridge University.

Closed source – Program code that's obfuscated but still usable. Only the company that made it can view, edit and share it on its own terms. Opposite of **open source**.

Cloud – A marketing term for someone else's computer. Users usually have no right to their **private data** on the cloud.

Cortana – **Narrow AI** exclusive to Windows 10. Uses all data present on the system.

Data mining – Gathering **private data** from naïve users through obscure means, such as Facebook tracking logged in users across websites through Like buttons.

Deep Blue – IBM's chess playing computer program that defeated then-best human player, Gary Kasparov, in 1996. Worked by **brute force**.

Deepfake – Video where faces have been digitally altered using **deep learning** and photos to make a realistic fake.

Deep learning – New name for **neural networks**.

Emergent – Property that appears (emerges) on its own from something we built. It is thought **super AI** is an emergent property of **general AI**, which is an emergent property of **narrow AI**.

Evergreen software – Shoddy computer program that requires constant updates to barely work.

Flippy – Caliburger's robotic burger flipping arm that can cook patties on its own, used for promotional purposes. Malfunctions all the time and needs constant maintenance.

GDPR – Comprehensive set of laws and policies instated May 25th, 2018 across the European Union. A serious attempt by EU to curb **Big Data** and **data mining**, naming the **right to be forgotten** as a fundamental right. Fines for obstinate companies go up to €20 million and more.

General AI – AI that has the curiosity and comprehension of a human. So far hasn't been created but is presumed to evolve to **super AI** very quickly.

Gray goo – Theoretical doomsday scenario in which haywire **nanobots** consume the entire Earth. Thought to be highly unlikely since all resources are finite.

Image recognition – Teaching **neural networks** to see and understand images like a human would.

Logic gates – Circuits that can take any number of inputs but always produce one output. Exist in several varieties and may be combined. Essential for making a computer.

Machine learning – Process that evolves a computer program and lets it experience the world like a living being would. Given enough **private data**, such computer program can predict user behavior trends. Opposite of **static programming**.

Mechanical Turk – Machine made in 1770 resembling a seated Turk sorcerer at a cabinet. Played chess at a very strong level but actually had a hidden operator within the cabinet. Destroyed in fire in 1840.

Metadata – Data on data, such as how long a phone call lasted. Has flimsy legal protections. When compiled in massive quantities exposes general behavior trends (see **Big Data**).

Michal Kosinski – Professor of psychology at Cambridge. Created a massively popular Facebook quiz in 2008. Gathered **private data** users voluntarily shared

and sold it to **Cambridge Analytica**.

Monte Carlo tree search – Computer **algorithm** that runs through moves in various turn-based games (checkers, chess, etc.) and gives them value based on how likely they are to win. May take an inordinate amount of time to check all moves in very complex games.

Nanobots – Robots the size of a nanometer (10^{-9} m) that can disassemble matter and create anything. Might lead to **gray goo** scenario. So far exist only in science fiction. Aka "nanites".

Narrow AI – AI that can do only one task. One example is autopilot in **Tesla**. Gradually becoming better and spreading everywhere.

Natural language processing – **Neural networks** working to parse words, sentences and ideas. Used in translation and automatic writing.

Neural networks – Computer programs combined together to resemble neurons in a living brain. Data is forwarded between nodes and slightly altered with each pass. Used in speech and **image recognition**.

Open source – Program code available to everyone to download, share, edit and make money on. Opposite of **closed source**.

Private data – Bits of data not meant for the public, such as the content of a phone call (see **Big Data**).

Right to be forgotten – The right of individuals to request their **private data** be deleted. May apply to a **search engine** hosting an embarrassing or false news article.

Search engine – Public facing side of a **narrow AI** users can search through. Contains information on behavior trends of its users.

Self-driving – Marketing term for **autopilot** cars. There are no actual self-driving cars yet and they're unlikely to appear within the next 50 years.

Shadow profile – Unauthorized tracking of users who attempt to guard their **private data**. Term first appeared with Facebook but is likely all social networks create shadow profiles since they aren't illegal.

Social engineering – Gaining the trust of employees in a company to hijack users' **private data**.

SpotMini – Advanced version of **Big Dog**. Has a robot arm where its head should be that can open doors.

Static programming – Programming software so it works out of the box. Opposite of **machine learning**.

Super AI – Godlike **AI** that might throw our civilization into chaos. Unknown when it might appear but speculated to quickly follow the appearance of **general**

AI.

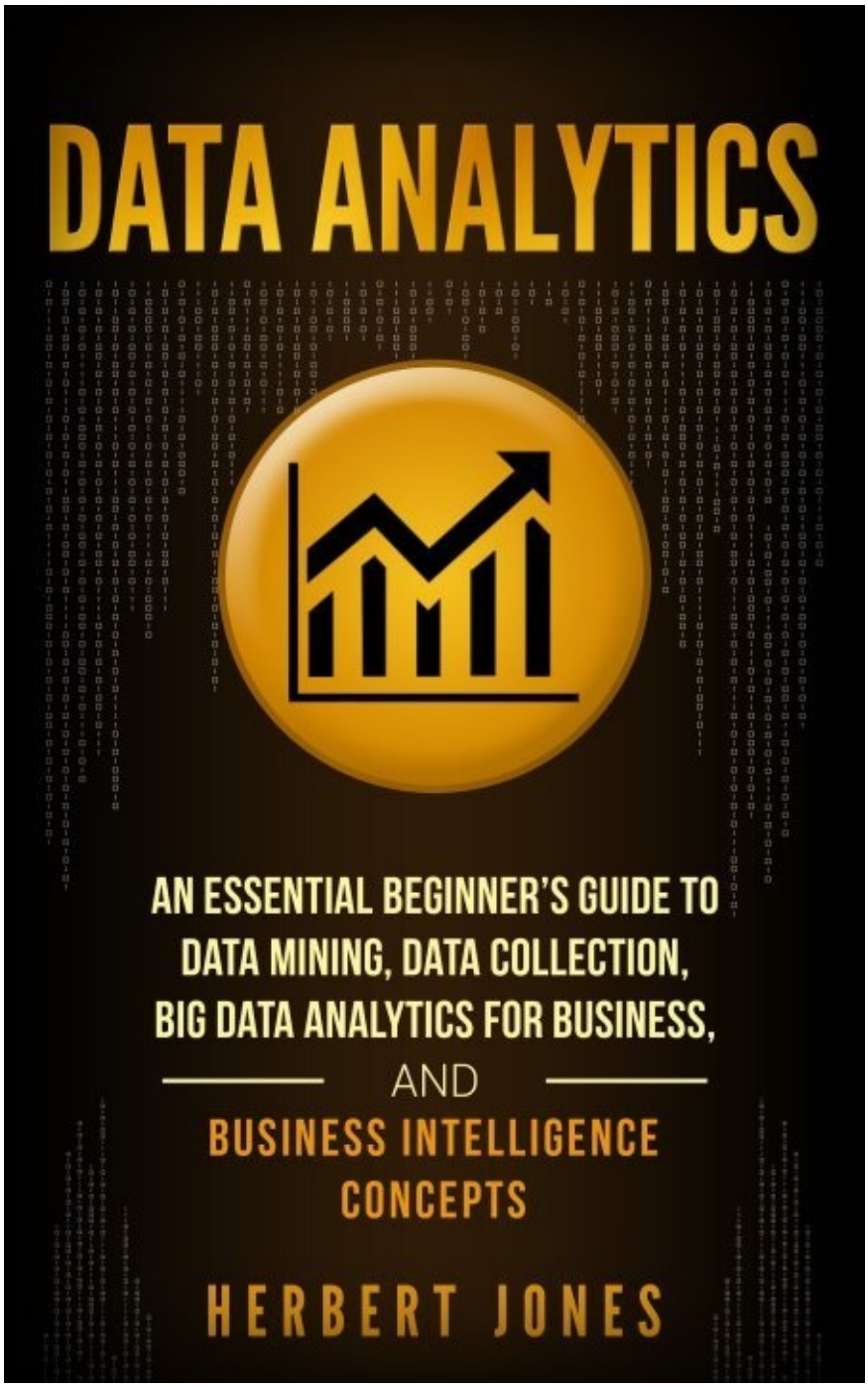
Supervised learning – **Machine learning** done under the auspices of a human teacher (compare to **unsupervised learning**).

Telemetry – Data related to usage of some program or device. For example, **Tesla** telemetry might show how many times any given driver has turned left in the past month.

Tesla – Electric car with **autopilot** capabilities. Requires driver attention at all times and is not self-driving. Highly sought after but still unreliable for mass adoption.

Unsupervised learning – **Machine learning** done without any human input, using only massive amount of data.

Check out another book by Herbert Jones



[Click here to check out this book!]

[1] https://www.eapoe.org/works/essays/maelzel.htm
[2] https://www.eia.gov/tools/faqs/faq.php?id=97&t=3
[3] https://www.popsci.com/technology/article/2009-11/neuron-computer-chips-could-overcome-power-limitations-digital
[4] https://www.wired.com/2016/01/in-a-huge-breakthrough-googles-ai-beats-a-top-player-at-the-game-of-go/
[5] https://arxiv.org/pdf/1412.1897v4.pdf
[6] https://www.sciencealert.com/a-man-who-lives-without-90-of-his-brain-is-challenging-our-understanding-of-consciousness
[7] https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160
[8] http://fortune.com/2013/01/07/teaching-ibms-watson-the-meaning-of-omg/
[9] https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/
[10] https://futurism.com/ray-kurzweil-ai-displace-humans-going-enhance/
[11] http://triblive.com/business/technology/13520920-74/aurora-ceo-chris-urmson-says-self-driving-tech-too-important-not-to-succeed
[12] http://money.cnn.com/2014/10/26/technology/elon-musk-artificial-intelligence-demon/index.html
[13] https://www.washingtonpost.com/news/the-switch/wp/2015/01/28/bill-gates-on-dangers-of-artificial-intelligence-dont-understand-why-some-people-are-not-concerned
[14] https://www.washingtonpost.com/news/speaking-of-science/wp/2014/12/02/stephen-hawking-just-got-an-artificial-intelligence-upgrade-but-still-thinks-it-could-bring-an-end-to-mankind
[15] https://www.forbes.com/sites/forbestechcouncil/2018/02/26/artificial-intelligence-will-take-your-job-what-you-can-do-today-to-protect-it-tomorrow/#771061bc4f27
[16] https://www.kioskmarketplace.com/blogs/will-restaurant-ordering-kiosks-replace-employees/
[17] https://www.youtube.com/watch?v=78-1MlkxyqI
[18] https://globalnews.ca/news/2888337/meet-sophia-the-human-like-robot-that-wants-to-be-your-friend-and-destroy-humans/
[19] http://www.dailymail.co.uk/sciencetech/article-3641468/Pepper-robot-finds-job-healthcare-friendly-droid-trialled-two-hospitals-Belgium.html
[20] https://www.yahoo.com/news/honda-demonstrates-version-asimo-humanoid-robot-074606276.html
[21] https://www.youtube.com/watch?v=W1czBcnX1Ww&feature=player_embedded
[22] https://www.youtube.com/watch?v=aFuA50H9uek
[23] https://www.youtube.com/watch?v=Ve9kWX_KXus
[24] https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1253&context=nulr
[25] https://storage.googleapis.com/sdc-prod/v1/safety-report/Safety%20Report%202018.pdf
[26] https://www.tesla.com/en_GB/videos/autopilot-self-driving-hardware-neighborhood-long?redirect=no
[27] https://www.mirror.co.uk/news/world-news/man-dies-tesla-electric-car-12540699
[28] http://www.sun-sentinel.com/local/broward/fort-lauderdale/fl-sb-engulfed-flames-car-crash-20180508-story.html
[29] https://www.youtube.com/watch?v=B2pDFjIvrIU
[30] http://www.alltrucking.com/faq/truck-drivers-in-the-usa/

[31] https://www.theguardian.com/technology/2016/jun/17/self-driving-trucks-impact-on-drivers-jobs-us
[32] https://www.theguardian.com/technology/2016/apr/07/convoy-self-driving-trucks-completes-first-european-cross-border-trip
[33] https://nypost.com/2018/05/25/amazon-blames-creepy-alexa-incident-on-unlikely-string-of-events/amp/
[34] https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740
[35] https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp
[36] https://gizmodo.com/facebook-reportedly-wants-to-use-ai-to-predict-your-fut-1825245517
[37] https://code.facebook.com/posts/1072626246134461/introducing-fblearner-flow-facebook-s-ai-backbone/
[38] https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win
[39] https://www.youtube.com/watch?v=yoN7LapRsKI
[40] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas
[41] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[42] https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691
[43] https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/
[44] https://www.microsoft.com/en-us/servicesagreement
[45] https://privacy.microsoft.com/en-us/privacystatement
[46] https://www.theatlantic.com/magazine/archive/2018/04/big-in-china-machines-that-scan-your-face/554075/
[47] https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html
[48] https://www.researchgate.net/publication/230827337_A_programmable_NOR-based_device_for_transcription_profile_analysis
[49] http://www.baen.com/Chapters/9781625791153/9781625791153___2.htm
[50] http://e-drexler.com/d/06/00/EOC/EOC_Chapter_1.html